

How we protect your company, layer by layer

We run IT for more than 80 companies in Romania, between 10 and 300 employees. For all of them, security comes in the same subscription as IT support. **Five layers of security we set up, run and answer for, with round-the-clock monitoring.**

Attacks come from two directions. The software guarding the endpoints sees nothing of the accounts, and the one guarding the accounts sees nothing of the endpoints.

ENDPOINTS

Laptops, desktops, servers, work phones

- Ransomware starting to encrypt files.

ACCOUNTS

Microsoft 365, passwords, browser sessions

- A sign-in from another country, at 4am.

Both reach the same analysts, on shift around the clock

They confirm it really is an attack, not routine activity, and stop it from spreading.

8 min

RESPONSE TIME

From the alert to the attack being stopped

24/7

SOC MONITORING

Security analysts on shift, nights and weekends included

100%

BACKUPS TESTED

Of the clients we manage, not merely taken

25 years

EXPERIENCE

With the same colleagues in Bucharest who know your network

ISO/IEC 27001:2022

Certificate RO231109006, externally audited yearly, verifiable in IAF CertSearch

Microsoft Solutions Partner

We run your Microsoft 365 environment directly

More than 80 companies

Between 10 and 300 employees, in Romania

Included in the subscription

Security sits inside the managed IT subscription

What changed in Romania. In 2025 the national cyber security authority reported a 353% rise in compromised accounts and a 153% rise in ransomware incidents.

NIS2 is transposed into Romanian law through Law 58/2024. If your company falls under it, security measures are no longer a choice, and the responsibility sits with management, not with the IT department.

The five layers of security, plus two optional ones

Each layer catches something different and none sees everything. What one misses, the next picks up. **The further down you go, the less the software does and the more a person does.** The last two are optional.

01

Files already known to be dangerous ANTIVIRUS

It blocks what already appears on the known-threat lists. It is the protection every company has, except that ours does not stay on the out-of-the-box settings: we configure it properly and check month after month, on every device, that it is still running.

ANALOGY *The list of known faces at the door.*

ENDPOINT

02

What happens on the endpoints EDR

It watches behaviour rather than files: which programs start, ransomware beginning to encrypt, the traces an attacker leaves to get back in. It can isolate the machine within seconds, but an analyst takes that decision.

ANALOGY *The motion sensors inside the building.*

ENDPOINT

03

Who signs in to the Microsoft 365 accounts, and what they do next ITDR

It learns what is normal for each account, then flags the deviations. Access from another country at four in the morning, stolen sessions, new rules hiding emails about invoices, an ordinary account suddenly gaining administrator rights.

ANALOGY *The doorman who checks the badge on the way in and watches what the person does once inside.*

ACCOUNTS

04

Somebody watching, around the clock SOC

The telemetry from layers 02 and 03 arrives together at the monitoring centre. An analyst decides whether it is a real attack or a false alarm, then acts: taking the machine off the network or locking the account.

ANALOGY *The dispatch room, staffed in shifts, around the clock.*

BOTH ZONES

05

Somebody who comes and fixes it YOUR IT SUPPORT TEAM

We check what the attacker touched before being stopped, clean the machine, reconnect it and write the incident report. This is where the chain closes, which is why it is last.

ANALOGY *The crew that turns up on site and puts everything back in order.*

BOTH ZONES

+

Every log, in one place SIEM

Layers 02 and 03 see only the endpoints and the accounts. This layer adds the records from Windows, the firewalls, the VPN and the other connected devices. With more sources, the same analysts can correlate more signals and catch earlier what would otherwise surface late. It also leaves a written record, kept for years, useful for an audit.

OPTIONAL

+

The people who click the links SAT · SECURITY AWARENESS TRAINING

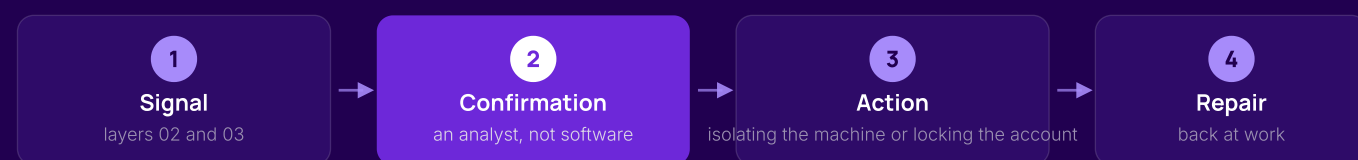
Short, interactive monthly training, followed by simulated phishing emails. The theory gets checked in practice: you see who learned it and who still needs help. It replaces no technical layer, but it stops some attacks before they start.

OPTIONAL

We set up all five, we run them and we answer for them. The last two are not part of the subscription by default, but we recommend them to most companies.

What happens, step by step

The order matters: **nothing is isolated before a person confirms it.** That way we do not stop the company for a false alarm.



If the alarm is false

- The analyst closes it and you never hear about it
- **Nobody is stopped from working**
- It stays written in your report

If the threat is real

- We take the computer off the network **within minutes**, after confirmation
- We lock the account and revoke its open sessions
- The rest of the company carries on, undisturbed

MTTR from the alert to the attack being stopped. Clean-up comes afterwards.

8 min

Our average, measured on every incident.

It includes the triage an analyst does, not only the automatic detection.

Eight minutes means an attack that starts at three in the morning is stopped before daybreak. By the time the first employee reaches the office, the incident is already closed. **This holds at any hour**, including nights, weekends and public holidays.

Want to know where you are exposed?

A free 45-minute assessment, online, with a written report afterwards. You pick the time, no obligation.

risksoft.eu/cybersecurity